Journal of Algebra **240,** 822–835 (2001)
doi:10.1006/jabr.2000.8741, available online at http://www.idealibrary.com on IDEAL®

Integer Polynomials with Roots mod p for all Primes p

Rolf Brandl

Mathematisches Institut, Am Hubland 12, D-97074 Würzburg, Germany

Communicated by G. Stroth

Received September 15, 2000

Let $f(X)$ be an integer polynomial which is a product of two irreducible factors. Assume that $f(X)$ has a root mod p for all primes p. If the splitting field of $f(X)$ over the rationals is a cyclic extension of the stem fields, then the Galois group of $f(X)$ over the rationals is soluble and of bounded Fitting length. Moreover, the fixed groups of the stem extensions are in, some sense, unique.

1. THE RESULTS

Let $f(X)$ be a monic integer polynomial over the integers. If one tries to factorize $f(X)$, one often looks at the reduction of $f(X)$ mod p for suitable primes p, decomposes $f(X)$ mod p, and then tries to say something about $f(X)$ over the integers. For example, if $f(X)$ is irreducible mod p for *some* prime p, then $f(X)$ is irreducible over the integers. However, there are irreducible polynomials that are reducible mod p for *all* primes p. See for example [1]. In some sense, these polynomials are particularly difficult to factorize. For more information on this topic, see [9].

Here, we are interested in the case when $f(X)$ even has a root mod p for all primes p. Clearly, this is the case when $f(X)$ has a linear factor. However, also the polynomial $h(X) = (X^3 - 2)(X^2 + X + 1)$ has this property. Now if $f(X)$ is irreducible with this property, then $f(X)$ has a linear factor (see [7] or [2]) and hence is linear. So the "first" case of interest is when $f(X)$ splits into a product of two irreducible factors over the integers as does $h(X)$. The following describes the Galois group of $f(X)$ in this case.

THEOREM A. *Let $f = f_1 f_2$ be a monic integer polynomial which is a product of two irreducible factors f_1, f_2. Assume that for every prime p the congruence $f(x) \equiv 0 \bmod p$ has an integer solution x (i.e., $f(X)$ has a root mod p*

0021-8693/01 $35.00

for all primes p). Let K be the splitting field of f over the rationals, and let ϑ_1, ϑ_2 be complex roots of f_1, f_2, respectively. Assume that for $i = 1, 2$ the Galois group of $K \mid \mathbb{Q}(\vartheta_i)$ is cyclic. Then the Galois group G of f over the rationals contains a series of normal subgroups $1 \leq F \leq R \leq G$ such that F is nilpotent, R/F is abelian, and G/R is cyclic. In particular, G is soluble.

In the situation of Theorem A, let U_i be the Galois group of $K \mid \mathbb{Q}(\vartheta_i)$ $(i = 1, 2)$. Using a result of Dedekind (see [1, Lemma 2]), the condition in Theorem A can easily be translated into a purely group-theoretical condition on the Galois group G. Indeed, G has a cyclic covering by the Galois groups U_i in the following sense.

DEFINITION. *Let $\mathfrak{X}$ be a class of groups. The finite group G has an $\mathfrak{X}$-covering if there exist $\mathfrak{X}$-subgroups U_1 and U_2 of G such that*

$$G = \bigcup_{g \in G} U_1^g \cup \bigcup_{g \in G} U_2^g \qquad (*)$$

If $\mathfrak{X}$ is the class of all cyclic, resp. nilpotent, groups, we shall say that G has a cyclic, resp. nilpotent, covering.

Hence Theorem A is a consequence of the next result that will be proved in the subsequent sections. Note that Theorem B depends on the classification of all finite simple groups.

THEOREM B. *Let G be a finite group.*

(a) *If G has a nilpotent covering, then G is soluble.*

(b) *If G has a cyclic covering, then $G/F(G)$ is metabelian. Moreover, $G/\gamma_\infty(G)$ is cyclic.*

As a consequence of Theorem B, a group with a cyclic covering is of Fitting length ≤ 3. It is not known to the author whether there is a bound for the Fitting length of groups with a nilpotent covering.

Note that the group G in Theorem A is soluble and hence occurs as the Galois group of some integer polynomial over the rationals. However, it is not clear whether one can choose this polynomial with the property that it has a root mod p for all primes p. Indeed, most of the construction in [1] works. However, the Frobenius Density Theorem (see [1, Lemma 1]) gives information only on the primes that do not divide the discriminant of the field. At least the symmetric group S_3, which obviously has a cyclic covering, occurs as a Galois group of the aforementioned polynomial $h(X)$. More generally, let $r \geq 3$ be a prime, and let $h_r(X) = (X^r - 2)\Phi_r(X)$, where Φ_r denotes the rth cyclotomic polynomial. Let p be a prime. If r does not divide $p - 1$, then 2 is an rth power in $GF(p)$, and so the first factor has a root mod p. If $r \mid p - 1$, then $GF(p)$ contains primitive rth roots of unity, and so Φ_r has a root mod p . Hence $h_r(X)$ has a root mod p for all

primes p, and so its Galois group, which is the Frobenius group of order $r(r-1)$, can be realized. This leaves us with the following inverse problem:

Conjecture. Assume that the finite group G has a cyclic covering. Does there exist an integer polynomial $f(X)$ with the properties mentioned in Theorem A and with Galois group G over the rationals?

The following example shows that, in general, the group G in Part b of Theorem B need not be metanilpotent.

EXAMPLE 1. Let N be an elementary abelian 2-group of order 8, and let $Q = [A]B$ be a Frobenius group where A and B are cyclic of order 7 and 3, respectively. Let $G = [N]Q$ be the natural split extension. Then G is of Fitting length three.

Let $U_1 = A$ and $U_2 = C_G(B)$. As $|C_N(B)| = 2$, we have that U_2 is a cyclic group of order 6. We claim that U_1, U_2 define a cyclic covering of G. Indeed, G has elements of order 1, 2, 3, 6, and 7, respectively. By Sylow's Theorem every element of order 7 is contained in some conjugate of U_1. Now U_2 contains an element of order 2. As all such are conjugate in G, the subgroup N of G is covered by conjugates of U_2. Also, U_2 contains elements of order 3, and by Sylow's Theorem, all such are covered by conjugates of U_2. Finally, let $x \in G$ be an element of order 6. Then $x \in C_G(x^2)$ and $o(x^2) = 3$. Hence $\langle x^2 \rangle$ is a Sylow 3-subgroup of G, and so we get $\langle x^2 \rangle^g = B$ for some element $g \in G$. Hence $x^g \in C_G(x^2)^g = C_G(B) = U_2$. This shows that U_1, U_2 define a cyclic covering of G.

The second example shows that the Fitting subgroup $F(G)$ of G can be nonabelian.

EXAMPLE 2. Let $q = 2^f$ where $f \geq 3$ is odd, and let G be the normalizer of a Sylow 2-subgroup N of the simple group $Sz(q)$ of Suzuki. Then $G = [N]Q$ where Q is a cyclic group of order $q-1$. Let U_1 be a cyclic subgroup of order 4 of N, and set $U_2 = Q$. We claim that U_1, U_2 define a cyclic covering of G. Note that the Fitting subgroup $N = F(G)$ is nonabelian.

Now G is a Frobenius group. Hence all elements in $G \backslash N$ belong to some conjugate of U_2. Moreover, it is known that all cyclic subgroups of order 4 of N are conjugate in G. (This follows for example from the fact that there are precisely two conjugacy classes of elements of order 4 in $Sz(q)$ and the Sylow 2-subgroups of $Sz(q)$ have trivial intersection with their conjugates.) Hence U_1, U_2 define a cyclic covering of G.

If U_1 and U_2 define a cyclic covering of the group G then, for all $x, y \in G$, also the conjugates U_1^x and U_2^y define a cyclic covering of G. The following shows that, apart from this, there is uniqueness of the covering subgroups of G up to conjugacy. Note that Theorem C has an obvious interpretation in the setting of Theorem A, which is somewhat lengthy to write down.

THEOREM C. *Let G be a noncyclic finite group with a covering by cyclic subgroups U_1, U_2. If subgroups V_1, V_2 define another cyclic covering of G, then there exist elements $x, y \in G$ such that $V_1 = U_1^x$, $V_2 = U_2^y$ or $V_1 = U_2^x$, $V_2 = U_1^y$.*

Proof. Let $U_i = \langle u_i \rangle$ $(i = 1, 2)$. By hypothesis, there exists an element $g \in G$ such that $u_1^g \in V_1$ or $u_1^g \in V_2$. We may assume $u_1^g \in V_1$. Let $V_1 = \langle v_1 \rangle$. As U_1, U_2 define a covering of G, there exists an element $h \in G$ such that $v_1^h \in U_1$ or $v_1^h \in U_2$.

If $v_1^h \in U_2$, then $U_1^{gh} \leq U_2$. But then G is covered by all conjugates of U_2. By [3, Sect. 26], it follows that $G = U_2$ is cyclic, a contradiction. This case does not occur. So we have $v_1^h \in U_1$. From this, we get $U_1^{gh} = \langle u_1^g \rangle^h \leq V_1^h \leq U_1$, and hence $V_1^h = U_1$. An analogous argument shows that V_2 is conjugate to U_2. ∎

If G is cyclic, then we can choose $U_1 = U_2 = V_1 = G$ and $V_2 = 1$. In this example, Theorem C is no longer valid. Also, if U_1, U_2 define a cyclic covering of a group G, then any two supergroups of U_1, U_2 also define a (not necessarily cyclic) covering. In Example 2 above, it is easy to construct two coverings of G by abelian groups U_1, U_2, V_1, V_2 which are nonconjugate in the sense of Theorem C.

Our notation follows that of [6] and [8]. In particular, a Frobenius group is not equal to 1. For a positive integer n, let $\pi(n)$ denote the set of all prime divisors of n and $\pi(G) = \pi(|G|)$ for a group G. For a prime p, we denote by $|G|_p$ the p-part of the order of G. In addition, $G = [N]Q$ means that G is a split extension of a normal subgroup N by a complement Q, and $X * Y$ denotes the central product of X and Y. All groups in this paper are finite.

2. THE MINIMAL COUNTEREXAMPLE (SOLUBLE CASE)

In this section, we prove Part b of Theorem B for soluble groups. The following simple observation on groups with a cyclic covering will be used without further mention.

LEMMA 1. *Assume that the finite group G has a covering by cyclic subgroups U_1 and U_2. Then*:

(a) *For every prime p, there are at most two conjugacy classes of subgroups of order p in G.*

(b) *For each normal subgroup N of G, the subgroups U_1N/N and U_2N/N of G/N define a cyclic covering of G/N.*

From Lemma 1, we immediately get one of the claimed properties of groups with a cyclic covering.

LEMMA 2. *Assume that the finite group G has a cyclic covering. Then $G/\gamma_\infty(G)$ is cyclic.*

Proof. Let U_1, U_2 be two cyclic subgroups that cover G. Let $\overline{G} = G/\gamma_\infty(G)$. Then $\overline{G}$ is covered by the cyclic groups $\overline{U}_1$ and $\overline{U}_2$. First assume that $\overline{U}_1 \neq \overline{G} \neq \overline{U}_2$. Then $\overline{U}_i$ is contained in some maximal subgroup $\overline{M}_i$ of $\overline{G}$ $(i = 1, 2)$. As $\overline{G}$ is nilpotent, $\overline{M}_i$ is normal in $\overline{G}$. Thus, $\overline{U}_i^x \subseteq \overline{M}_i$ for all $x \in \overline{G}$ and $i = 1, 2$. This implies that $\overline{G} = \overline{M}_1 \cup \overline{M}_2$ is the union of two proper subgroups, a contradiction. So $\overline{U}_i = \overline{G}$ for some index i, and $\overline{G}$ is cyclic. ∎

Let G be a finite soluble group with a cyclic covering as in $(*)$. We try to prove that $G/F(G)$ is metabelian. For this, we need some information on the class of all such groups.

LEMMA 3. *The class $\mathcal{K}$ of all finite groups G such that $G/F(G)$ is metabelian is a saturated formation.*

Proof. Clearly, $\mathcal{K}$ is a formation. Let G be a group such that $G/\Phi(G) \in \mathcal{K}$. Let $N/\Phi(G)$ be a normal subgroup of $G/\Phi(G)$ such that G/N is metabelian. By [8, p. 270], we get that N is nilpotent, and hence we have $G \in \mathcal{K}$. ∎

In the remainder of this section, let G be a soluble counterexample of least possible order to Part b of Theorem B. If we speak about U_1, U_2 without any explanation, we shall tacitly assume that these are cyclic covering subgroups of our group G.

LEMMA 4. *We have $G = [N]Q$, where N is the unique minimal normal subgroup of G (assume that N is a p-group) and Q is nilpotent-by-metabelian. Moreover, $C_G(N) = N$ and $Q/\gamma_\infty(Q)$ is cyclic.*

Proof. By Lemma 1b, every factor group of G has a cyclic covering. Hence, if G has two distinct minimal normal subgroups N_1, N_2, by the minimality of G the factor groups G/N_1 and G/N_2 are $\mathcal{K}$-groups. As $\mathcal{K}$ is a formation, this yields $G \in \mathcal{K}$, a contradiction. Hence G has a unique minimal normal subgroup N, say.

If $\Phi(G) \neq 1$, then the above implies $N \leq \Phi(G)$. Moreover, $G/\Phi(G)$ is a $\mathcal{K}$-group. By Lemma 3, the class $\mathcal{K}$ is a saturated formation, and so we get the contradiction $G \in \mathcal{K}$. Thus, $\Phi(G) = 1$, and hence N has a complement Q in G. Moreover, $Q \cong G/N \in \mathcal{K}$.

As G is not nilpotent, we have $N \leq \gamma_\infty(G)$. Thus, $\overline{G} = G/\gamma_\infty(G) \cong Q/\gamma_\infty(Q)$ is cyclic by Lemma 2. ∎

We collect some information about extensions of elementary abelian p-groups by elementary abelian r-groups. Part a of the following result is well known.

LEMMA 5. *Let $H = [N]A$, where A is an elementary abelian r-group for some prime r of rank t, say, acting faithfully on the elementary abelian p-group N with $p \neq r$. Assume that $C_N(A) = 1$. Then*

(a) *$H = H_1 \times \cdots \times H_t$ is a direct product of t Frobenius groups of the form $H_i = [N_i]A_i$, where $N_i \leq N$ is the Frobenius kernel of H_i and $A_i \leq A$ is its complement.*

(b) *There exist elements $n \in N$ and $a \in A$ such that $C_H(n) = N$ and $C_H(a)$ is an elementary abelian r-group.*

(c) *If $r \geq 3$ and $t \geq 2$, then there exist two distinct cyclic subgroups $\langle a \rangle, \langle b \rangle$ of A such that $C_N(a) = 1 = C_N(b)$.*

(d) *If $r = 2$ and $t \geq 3$, then there exist elements $x, y, z \in A$ of order 2 such that $C_N(x)$, $C_N(y)$, and $C_N(z)$ have pairwise distinct orders.*

Proof. (b) For $1 \leq i \leq t$, choose $n_i \in N_i \setminus \{1\}$ and $a_i \in A_i \setminus \{1\}$. Moreover, let $n = n_1 \cdots n_t$ and $a = a_1 \cdots a_t$.

Let $x = md \in C_H(n)$, where $m \in N$ and $d \in A$. Then $n = n^x = n^d$. This implies $n_i = n_i^d$ for all i, whence $d = 1$ and $x \in N$. This shows $C_H(n) = N$.

Finally, we have $C_H(a) \geq A$. By Dedekind's Lemma, we get $C_H(a) = [C_N(a)]A$. Now the choice of a guarantees that $C_N(a) = 1$, and hence $C_N(a) = A$ is an elementary abelian r-group.

(c) Let $a_1, \ldots, a_t, a$ be as in the proof of Part b, and set $b = a_1^{-1} \cdot a_2 \cdots a_t$. Then $C_N(a) = 1 = C_N(b)$. Moreover, as $r \neq 2$ and $t \geq 2$, we have $\langle a \rangle \neq \langle b \rangle$.

(d) Let $a_1, \ldots, a_t$ be as in the proof of Part b. As $t \geq 3$, we can form the elements $x = a_1 a_2 a_3$, $y = a_1 a_2$, and $z = a_1$. It is straighforward to check that these have the required property. ∎

The proof of our theorem depends on a study of the action of the complement Q in Lemma 4 on the minimal normal subgroup N. We first look at elementary abelian normal subgroups of Q.

LEMMA 6. *Let G be as in Lemma* 4, *and let A be an elementary abelian normal subgroup of Q. Then*:

(a) *A is cyclic, and $H := [N]A$ is a Frobenius group.*

(b) *All subgroups of order p of N are conjugate in G.*

Proof. By Lemma 4, the subgroup $H = NA$ of G satisfies the hypothesis of Lemma 5. Let n be as in Lemma 5b. We may assume that n is contained in a conjugate U_1^g of U_1. Clearly, we may assume $n \in U_1$.

As U_1 is abelian, we have $U_1 \leq C_G(n)$. This implies $U_1 \cap H \leq C_G(n) \cap H = C_H(n) = N$. As U_1 is cyclic, we get $|U_1 \cap H| = p$.

Let a be as in Lemma 5b. Then no conjugate of a in G can have a fixed point not equal to 1 on N. If $a \in U_1^h$ for some $h \in G$, then $a \in C_G(n)^h = C_G(n^h)$, and so $C_N(a) \neq 1$, a contradiction. Hence a is contained in some conjugate of U_2. We may assume $a \in U_2$. As above, this yields $U_2 \leq C_G(a)$, so that $U_2 \cap H \leq C_H(a)$ is an elementary abelian r-group. As U_2 is cyclic, we get $|U_2 \cap H| = r$.

If H is not Frobenius, then H contains an element x of order pr. But $U_i \cap H$ is of prime order, and so x cannot be contained in any conjugate of U_i $(i = 1, 2)$, a contradiction. This proves Part a.

For Part b, let S be a subgroup of order p of N. If S were conjugate to a subgroup of U_2, then we would have $U_2 \cap N \neq 1$. But $|U_2 \cap H| = r$, a contradiction. Thus S is conjugate to a subgroup of U_1. As U_1 is cyclic, it has precisely one subgroup of order p, and so all subgroups of order p of N are conjugate in G. ∎

The following result contains information on the conjugacy of certain subgroups of Q:

LEMMA 7. *Let G be as in Lemma* 4, *and let $F = F(Q)$ be the Fitting subgroup of Q. If r is a prime dividing the order of F, then Q contains precisely one normal subgroup R of order r. Moreover, all subgroups not equal to R of order r in Q are conjugate in Q.*

Proof. As r divides the order of F, the group F contains a characteristic elementary abelian r-subgroup $R \neq 1$. Thus, R is normal in Q. From Lemma 6a, we infer that R is cyclic of order r.

Now Q, by Lemma 1b, can be covered by two cyclic subgroups V_1, V_2. Without loss, we may assume that $R \leq V_1^x$ for some $x \in Q$. As R is normal in Q, we get $R \leq V_1$. Now let R' be a subgroup of Q of order r with $R' \neq R$. If $R' \leq V_1^y$ for some $y \in Q$, then as V_1 is cyclic we would have $R' = R^y = R$. But this is against the choice of R'. So R' is conjugate to a subgroup of V_2. As V_2 is cyclic, this subgroup is uniquely determined, and hence all the aforementioned subgroups R' of Q are conjugate in Q. ∎

The following result collects some preliminary results on the Sylow subgroups of the Fitting subgroup of Q:

LEMMA 8. *Let G be as in Lemma* 4, *and let $F = F(Q)$. Then*:

(a) *All Sylow r-subgroups of F for primes $r \neq 2$ are cyclic.*

(b) *Every abelian 2-subgroup of F can be generated by ≤ 2 elements.*

Proof. (a) Let R be as in Lemma 7. If $O_r(F)$ were noncyclic, we could by [6, p. 199] choose a subgroup S of order r in F with $S \neq R$ (here, we

use $r \neq 2$). Consider the subgroup $V = \langle R, S\rangle = R \times S$. By Lemma 7, all subgroups not equal to R of order r of V are conjugate in Q.

Now by [6, p. 188] there exists a subgroup R^* of V of order r such that $C_N(R^*) \neq 1$. As $C_N(R) = 1$ and $R \trianglelefteq Q$, all subgroups $R^{**} \neq R$ of order r of V satisfy $C_N(R^{**}) \neq 1$. By Lemma 5c, applied to the subgroup $[N]V$ of Q, we get a contradiction. Thus the Sylow r-subgroup of F is cyclic.

(b) Otherwise, there exists an elementary abelian subgroup A of F of order 8. Let R be as in Lemma 7. By Lemma 7, all subgroups not equal to R of order 2 of A are conjugate in Q. This, however, contradicts Lemma 5d. ∎

We now describe the Sylow 2-subgroup of $F(Q)$.

LEMMA 9. *Let G be as in Lemma* 4, *let $F = F(Q)$, and let T be a Sylow 2-subgroup of F. Then either T is cyclic, dihedral, quasidihedral, a generalized quaternion group, or a central product of a quaternion group with a dihedral group of order* 8.

Proof. Note that by Lemma 8, every elementary abelian subgroup of T has order ≤ 4. By [8, p. 355], an extraspecial group of order $2^{2m+1} > 8$ which is nonisomorphic to the group $X = \mathbb{D}_4 * Q_8$ contains elementary abelian subgroups of order 8. Hence every extraspecial subgroup of T either has order 8 or is isomorphic to X.

Every abelian characteristic subgroup A of T is normal in Q. By Lemma 6a, all such groups A are cyclic. A result of Hall (see [8, p. 357]) gives the structure of T. We deal with the various cases.

If T is extraspecial, then by the above we must have $|T| = 8$ or $T \cong X$. Thus, the cases (1) and (2) of [8, p. 357] are dealt with.

Now, let $T = P * S$ be, as in [8, p. 357], the central product of an extraspecial 2-group P with a group S which is cyclic, generalized quaternion, or quasidihedral.

If S is cyclic (clearly of order ≥ 4), then T contains elements $f_1 \in P, f_2 \in S$ of order 4 such that $f_1 \notin Z(T)$ and $f_2 \in Z(T)$. Hence these elements cannot be conjugate to an element of *the same* covering subgroup U_i. Note that $f_1^2 = f_2^2$ and hence the involutions of U_1 and U_2 are conjugate. In particular, all involutions of T are conjugate in Q. However, $Z(T)$ is cyclic, so that T is either cyclic or a quaternion group of order 8.

Finally, let S be generalized quaternion or quasidihedral. If $|S| \geq 16$, then T contains elements $f_1 \in P, f_2 \in S$ of order 4 such that $f_2 = t^2$ is a square of an element $t \in T$, but f_1 is not. Hence f_1 is not conjugate to f_2 or f_2^{-1}. In particular, these elements cannot be conjugate to an element of the same covering subgroup. As above, we get a contradiction. Hence $|S| = 8$ and T is extraspecial. This case has already been dealt with. The assertion is proved. ∎

Proof of Theorem B, Part b (Soluble Case). Let G be a counterexample of least possible order. Then G has the structure as in Lemma 4, Lemma 8, and Lemma 9. We show that $F = F(Q)$ is cyclic. For this, we consider the Sylow 2-subgroup T of F.

Note that $Q/C_Q(F)$ is isomorphic to a subgroup of $\mathrm{Aut}(F)$. First, assume that T is neither a quaternion group of order 8 nor the group $\mathbb{D}_4 * Q_8$. We show that $Q/C_Q(F)$ is nilpotent. By the structure of T given in Lemma 9, the automorphism group $\mathrm{Aut}(T)$ is nilpotent. The Sylow subgroups of odd order of F are cyclic by Lemma 8, and hence their automorphism group is abelian. As F is nilpotent, we get that $\mathrm{Aut}(F)$ is nilpotent, whence $Q/C_Q(F)$ is nilpotent. From Lemma 2, we infer that $Q/C_Q(F)$ is cyclic.

As Q is soluble, we have $C_Q(F) \leq F$, so $C_Q(F) = Z(F)$. From this, we can conclude that $F/Z(F)$ is cyclic, whence F is abelian. Thus, by Lemma 6a, we have that F is cyclic. In this case, $Q/F = Q/C_Q(F)$ is abelian (even cyclic by Lemma 2) as well, but then G is not a counterexample any more.

This leaves us with two cases. First, let T be a quaternion group of order 8. Let $x \in T$ be an element of order 4. We may assume $x \in U_1$. As Q acts irreducibly on N and $x^2 \in Z(Q)$, we have $C_N(x^2) = 1$, and so we get $C_N(x) = 1$. As U_1 is abelian, this implies $U_1 \cap N = 1$.

If the automorphism group induced by Q on T is a 2-group, then we can conclude as in the first part of the proof. Otherwise, there exists an element $y \in Q$ which induces on T an automorphism of order 3. We may assume that y is of odd order. Now consider the element $z = yx^2$. If z is contained in some conjugate of U_1, say $z^g \in U_1$ for some $g \in G$, then z^g centralizes x. But this is against the choice of y. Thus, we have $z^g \in U_2$ for some $g \in G$. As $U_1 \cap N = 1$, we must have $U_2 \cap N \neq 1$. But then every element in U_2 has a nontrivial fixed point on N. In particular, we have $C_N(z^g) \neq 1$. As y is of odd order, the element x^2 is a power of z, and we get the contradiction $C_N(x^2) \neq 1$. This case does not occur.

Finally, let $T \cong \mathbb{D}_4 * Q_8$. Set $Z(T) = \langle w \rangle$. By Lemma 7, all involutions of T not equal to w are conjugate in Q. As T contains 11 involutions, we see that 10 divides $|Q|$ and hence there exists an element $g \in Q$ of order 5^k ($k \geq 1$) acting nontrivially on T.

We may assume $U_2 \cap N \neq 1$. Then every element of U_2 has a nontrivial fixed point on N. As $C_N(w) = 1$, the element gw of order $2 \cdot 5^k$ acts fixed point freely on N, and hence some of its conjugates are contained in U_1. Let $f \in T$ be an element of order 4. As $f^2 = w$ and $C_N(w) = 1$, we get that U_1 contains some conjugate of f. As U_1 is cyclic, gw centralizes some conjugate of f. In particular, the automorphism φ induced on T by gw centralizes an element of order 4 of T. However, $T/\langle w \rangle$ is elementary abelian of order 16, and hence φ acts irreducibly on this quotient. This is a final contradiction. ∎

3. NONSOLUBLE GROUPS

By the preceding section, it remains to show that groups with a nilpotent covering are soluble. We first determine the structure of minimal counterexamples. To make induction work, we have to modify the notion of nilpotent coverings. Indeed, we have to allow conjugacy by all automorphisms of the group G rather than just the inner automorphisms considered up to now.

DEFINITION. *Let $\mathscr{X}$ be a class of groups. The finite group G has an $\mathscr{X}$-covering under automorphisms if there exist subgroups U_1 and U_2 of G such that U_1 and U_2 are $\mathscr{X}$-groups and*

$$G = \bigcup_{\alpha \in \mathrm{Aut}(G)} \alpha(U_1) \cup \bigcup_{\alpha \in \mathrm{Aut}(G)} \alpha(U_2). \qquad (*)$$

If $\mathscr{X}$ is the class of all cyclic (resp., nilpotent) groups, we shall say that G has a cyclic (resp., nilpotent) $\mathrm{Aut}(G)$-covering.

We want to show that groups with an $\mathscr{X}$-covering under automorphisms for "nice" classes $\mathscr{X}$ are soluble. The following reduces the problem to simple groups.

PROPOSITION 10. *Let $\mathscr{X}$ be closed with respect to forming subgroups and quotients. If there exists a nonsoluble group with an $\mathscr{X}$-covering under automorphisms, then there exists a simple group with this property.*

Proof. Let G be a nonsoluble group of least possible order that has an $\mathscr{X}$-covering under automorphisms. We first show that G is characteristically simple. Otherwise, we can choose a proper characteristic subgroup C of G.

Let U_1, U_2 be as in the above definition. Then, obviously, G/C is covered by U_1C/C and U_2C/C under automorphisms. As $\mathscr{X}$ is closed by taking quotients, we have $U_iC/C \in \mathscr{X}$ for $i = 1, 2$. By minimality, G/C is soluble.

Now let $V_i = U_i \cap C$ $(i = 1, 2)$. We show that C is $\mathrm{Aut}(C)$-covered by V_1, V_2. Indeed, let $c \in C$. By hypothesis, there exists $\alpha \in \mathrm{Aut}(G)$ such that $\alpha(c) \in U_i$ for some index i. Now $\alpha(c) \in C$, and α is an automorphism of C. Thus, $\alpha(c) \in V_i$. As $\mathscr{X}$ is closed by taking subgroups, we have $V_1, V_2 \in \mathscr{X}$. By minimality, C is soluble. Hence G is soluble against the choice of G. Thus, G is characteristically simple.

Hence $G = E \times \cdots \times E$ is a direct product of t copies of a nonabelian simple group E. Denote by π the projection of G onto its first direct factor, and let $W_i = \pi(U_i)$ $(i = 1, 2)$. As $\mathscr{X}$ is closed by taking quotients, we have $W_1, W_2 \in \mathscr{X}$.

We show that for every element $g \in E$ there exists an automorphism β of E such that $\beta(g) \in W_i$ for some index i. Let $x = (g, g, \ldots, g) \in G$. By hypothesis, there exists an automorphism α of G such that $\alpha(x) \in U_i$ for some index i. By the well-known structure of the automorphism group of G,

we have $\alpha(x) = (\alpha_1(g), \ldots, \alpha_t(g))$, where $\alpha_1, \ldots, \alpha_t$ are automorphisms of E. In particular, we have $\alpha_1(g) = \pi(\alpha(x)) \in \pi(U_i) = W_i$. This shows that W_1, W_2 define an $\mathcal{X}$-covering under automorphisms of E. By minimality of G, we have that $G = E$ is simple. ∎

In view of Proposition 10, we now exclude the finite simple groups. Here, some properties of the prime graph of a finite group will be used. For its definition and basic properties, see [11]. The following elementary result will be the key for the study of finite simple groups:

LEMMA 11. *Let G be a group with a nilpotent* $\mathrm{Aut}(G)$*-covering.*

(a) *The prime graph of G has at most two connected components.*

(b) *Let π be a set of primes. If G contains an element x such that $C_G(x)$ is a π-group, then one of the covering subgroups is a π-group.*

(c) *Assume that for some prime p there are nonidentity elements $x, y \in G$ such that $C_G(x)$ is a p-group and $C_G(y)$ is a p'-group. Then every element of G is a p-element or a p'-element.*

Proof. Let U_1, U_2 be nilpotent subgroups of G that cover G under automorphisms.

(a) Let $\pi_e(X)$ denote the set of all orders of elements in the group X. The hypothesis on G yields $\pi_e(G) = \pi_e(U_1) \cup \pi_e(U_2)$. Now the prime graphs of U_1 and U_2 are connected, and hence the prime graph of G has at most two connected components.

(b) We may assume that $x \in U_1$. Clearly, $Z(U_1) \leq C_G(x)$, and so $Z(U_1)$ is a π-group. As U_1 is nilpotent, we see that U_1 must be a π-group.

(c) By Part b, we may assume that U_1 is a p-group and U_2 is a p'-group. As every element of G is contained in a conjugate of U_1 or U_2, the result follows. ∎

We now deal with the various types of simple groups separately. The following excludes the sporadic groups.

LEMMA 12. *No sporadic simple group G has a nilpotent* $\mathrm{Aut}(G)$*-covering.*

Proof. Let p be the largest prime divisor of the order of G. An inspection of [5] shows that every subgroup of G of order p is self-centralizing. So one of the covering subgroups, U_1, say, is of order p. All elements of order not equal to p are thus $\mathrm{Aut}(G)$-conjugate to some element of U_2. Let e be the least common multiple of all orders not equal to p of elements that occur in G. As U_2 is nilpotent, it must contain an element or order e. An inspection of [5] shows that this is not the case, a contradiction. ∎

The next result deals with the alternating groups.

LEMMA 13. *No alternating group* $G = A_n$ $(n \geq 5)$ *admits a nilpotent* $\mathrm{Aut}(G)$*-covering.*

Proof. First, let n be odd. Then G contains an n-cycle x, and we have $|C_G(x)| = n$. By Lemma 11b, one of the covering subgroups, U_1, say, is a $\pi(n)$-group. Similarly, G contains a product y of two disjoint cycles of length $(n-1)/2$, and $|C_G(y)|$ divides $2\big((n-1)/2\big)^2$. As n and $n-1$ are coprime, Lemma 11b implies that U_2 is a $\pi(n-1)$-group.

Now by Bertrand's Postulate (see for example [2, Lemma 3.1]), for $n \geq 5$, $n \neq 6$, there exists a prime p with $\frac{n}{2} < p \leq n-2$. It follows that p divides neither $|U_1|$ nor $|U_2|$. Hence a cycle of length p cannot be conjugate to any element of U_1 or U_2, a contradiction.

The case when $n \neq 6$ is even is similar. For $n = 6$ note that G does not contain any element of order 6. ∎

The following two lemmas show that all simple groups of Lie type satisfy the hypothesis of Lemma 11c.

PROPOSITION 14. *Let G be a simple group of Lie type in characteristic p. Then G contains an element u such that $C_G(u)$ is a p-group.*

Proof. By [4, (1.11), (1.17), and (1.19)], we can choose a simple algebraic group H of adjoint type and a Frobenius map F of H such that the group $\widehat{H} = H^F$ of fixed points in H under F satisfies $O^{p,p'}(\widehat{H}) \cong G$. As H is a connected reductive group, by [4, Prop. 5.1.7] there exists a regular unipotent element $u \in \widehat{H}$. Now $Z(H) = 1$ as H is of adjoint type, and by [4, (5.1.5)] the centralizer $C_H(u)$ does not contain any semisimple element not equal to 1. Therefore, $C_{\widehat{H}}(u)$ is a p-group. Now $u \in O^{p,p'}(\widehat{H}) \cong G$, and so the lemma holds unless G is of type $B_2(2)'$, ${}^2F_4(2)'$, $G_2(2)'$, or ${}^2G_2(3)'$. If G is one of these exceptions, an inspection of [5] shows that the result is also true in these cases. ∎

PROPOSITION 15. *Let G be a simple group of Lie type in characteristic p. Then G contains an element s such that $C_G(s)$ is a p'-group.*

Proof. For the groups $B_2(2)'$, ${}^2F_4(2)'$, $G_2(2)'$, and ${}^2G_2(3)'$, the result is clear from [5], so we may exclude these groups.

As in the proof of Proposition 14, we can choose a simple algebraic group H of simply connected type and a Frobenius map F of H such that the group $\widehat{H} = H^F$ of fixed points of F in H satisfies $\widehat{H}/Z(\widehat{H}) \cong G$. By [4, 1.18] we get that $\widehat{H}$ contains a (B, N)-pair. Let St be the Steinberg character of $\widehat{H}$ as defined in [4, 6.2]. By [4, 6.5.9], we have $\mathrm{St}(g) = \epsilon_H \epsilon_{C(g)^o} |C_{\widehat{H}}(g)|_p$ if g is semisimple, and $\mathrm{St}(g) = 0$ otherwise. In particular, $Z(\widehat{H})$ is contained

in the kernel of St, and hence it induces a complex character of G. From [4, 6.2.2], we infer that St is irreducible.

Let C be a set of representatives for the conjugacy classes of G and C_s be a set of representatives for all semisimple classes of G. The orthogonality relations imply that

$$\begin{aligned}|G| &= \sum_{g\in G} \mathrm{St}(g)\overline{\mathrm{St}(g)}\\ &= \sum_{g\in C} [G : C_G(g)] \cdot \mathrm{St}(g)\,\mathrm{St}(g)\\ &= \sum_{g\in C_s} [G : C_G(g)] \cdot |C_G(g)|_p{}^2\\ &= \sum_{g\in C_s} [G : C_G(g)]_{p'} \cdot |G|_p \cdot |C_G(g)|_p.\end{aligned}$$

After division by $|G|_p$, we get

$$|G|_{p'} = \sum_{g\in C_s} [G : C_G(g)]_{p'} \cdot |C_G(g)|_p.$$

As the left-hand side is a p'-number, there must be an element $s \in C_s$ with $|C_G(s)|_p = 1$, as claimed. ∎

The following shows that almost none of the simple groups of Lie type satisfies the conclusion of Lemma 11c.

LEMMA 16. *Let G be a simple group of Lie type defined over a field with $q = p^f$ elements. If G is not $A_1(q)$, ${}^2B_2(q)$, $A_2(2)$, $A_2(4)$, ${}^2G_2(3)'$, or $B_2(2)'$, then G contains an element whose order is neither a power of p nor a p'-number.*

Proof. Let Δ be the (twisted) Dynkin diagram of G. Suppose that Δ contains at least three nodes. As Δ does not contain any triangle, there are two nodes i_1 and i_2 which are not connected with each other. Let $J = \{i_1, i_2\}$, and let P_J be the parabolic subgroup corresponding to J. Then a Levi complement of P_J contains elements of "mixed" order. Therefore, Δ contains at most two nodes.

In the rank 1 case, first let $G = {}^2A_2(q)$. Then G contains a subgroup $(q+1)/(q+1,3) * SL(2,q)$. As $q > 2$, we have thus found elements of mixed order. The group ${}^2G_2(q)$ has a subgroup ${}^2G_2(3) \cong SL(2,8) : 3$, which contains elements of order 6.

In the rank 2 case, first let G be of type $A_2(q)$. Then a Levi complement to a maximal parabolic subgroup contains a subgroup of type $(q-1)/(q-1,3) * SL(2,q)$. Therefore, if $q \notin \{2,4\}$, we get elements of mixed order. The groups $B_2(q)$ and $G_2(q)$ contain subgroups of type

$A_1(q) * A_1(q)$, and ${}^2F_4(q)$ contains ${}^2F_4(2)'$, which by [5] has elements of order 6. The group ${}^3D_4(q)$ contains a $G_2(q)$, and ${}^2A_3(q)$ contains a ${}^2A_2(q)$. In the remaining case ${}^2A_3(2)$, we see elements of order 6 in a maximal parabolic. ∎

Proof of Theorem B (Nonsoluble Case). By way of contradiction, assume that there exists a nonsoluble group with a nilpotent covering. By Proposition 10, there exists a simple group G with this property. By the classification, Lemmas 12 and 13, we see that G is of Lie type in characteristic p, say. By Lemmas 14 and 15, the group G satisfies the hypothesis of Lemma 11c. Thus, Lemma 16 implies that G is $A_1(p^f)$, ${}^2B_2(p^f)$, $A_2(2)$, $A_2(4)$, ${}^2G_2(3)'$, or $B_2(2)'$.

The groups $A_1(p^f)$ are ruled out by an inspection of Dickson's list (see [8, p. 213f]). By [10] and [11], the groups ${}^2B_2(p^f)$, $A_2(2)$, and $A_2(4)$ have at least three prime graph components, but this is against Lemma 11a. Finally, the groups ${}^2G_2(3)' \cong A_1(8)$ and $B_2(2)' \cong A_6$ have already been ruled out. We have arrived at a final contradiction. ∎

ACKNOWLEDGMENT

The author is grateful to the referee for greatly improving upon the treatment of the simple groups.

REFERENCES

1. R. Brandl, Integer polynomials that are reducible modulo all primes, *Amer. Math. Monthly* **93** (1986), 286–288.
2. R. Brandl, D. Bubboloni, and I. Hupp, Polynomials with roots mod p for all primes p, *J. Group Theory* **4** (2001), 233–239.
3. W. Burnside, "Theory of Groups of Finite Order," 2nd ed., Dover, New York, 1955.
4. R. W. Carter, "Finite Groups of Lie Type–Conjugacy Classes and Complex Characters," Wiley–Interscience, Chicester, 1985.
5. J. H. Conway *et al.,* "Atlas of Finite Groups," Clarendon Press, Oxford, 1985.
6. D. Gorenstein, "Finite Groups," Harper & Row, New York/Evanston/London, 1968.
7. I. Hupp, "Polynome, die modulo jeder Primzahl eine Nullstelle besitzen," Diplomarbeit, Würzburg, 1991.
8. B. Huppert, "Endliche Gruppen," Vol. I, Springer-Verlag, Berlin/New York/Heidelberg, 1967.
9. E. Kaltofen, D. R. Musser, and B. D. Saunders, A generalized class of polynomials that are hard to factor, *SIAM J. Comput.* **12** (1983), 473–483.
10. A. S. Kondrat'ev, Prime graph components of finite simple groups, *Math. USSR Sb.* **67** (1990), 235–247.
11. J. S. Williams, Prime graph components of finite groups, *J. Algebra* **69** (1981), 487–513.